The Web's dark side grows darker

Spam, bots and other malicious gremlins gear up for a busy 2007

By BRIAN KREBS, Special to The Washington Post
Posted Sunday, December 31, 2006

WASHINGTON -- Call it the "year of computing dangerously."

Computer security experts say 2006 saw an unprecedented spike in junk e-mail and sophisticated online attacks from increasingly organized cyber crooks. These attacks were made possible, in part, by a huge increase in the security holes identified in widely used software products.

Few Internet security watchers believe 2007 will be any brighter for the millions of fraud-weary consumers already struggling to stay abreast of new computer security threats and avoiding clever scams when banking, shopping or just surfing online.

One of the best measures of the rise in cyber crime this year is spam. More than 90 percent of all e-mail sent online in October was unsolicited junk mail messages, according to Postini, a San Carlos, Calif.-based e-mail security firm. The volume of spam shot up 60 percent in the past two months alone.

As a result, network administrators are not only having to deal with considerably more junk mail, but the image-laden messages also require roughly three times more storage space and Internet bandwidth for companies to process than text-based e-mail, said Daniel Druker, Postini's vice president of marketing. "We're getting an unprecedented amount of calls from people whose e-mail systems are melting down under this onslaught," Druker said.

Spam volumes are often viewed as a barometer for the relative security of the Internet community at large, in part because most spam is relayed via "bots," a term used to describe home computers that online criminals have compromised surreptitiously with a computer virus or worm. The more compromised computers that the bad guys control and link together in networks, or "botnets," the greater volume of spam they can blast onto the Internet.

At any given time, 3 million to 4 million bots are active on the Internet, according to Gadi Evron, a botnet expert. "Botnets have become the moving force behind organized crime online, with a low-risk, high-profit calculation," Evron said. He estimated that organized criminals would earn about $2 billion this year through phishing scams, which involve the use of spam and fake Web sites to trick computer users into disclosing financial and other personal data. Criminals also seed bots with programs that can record and steal usernames and passwords from compromised computers.

"With botnets we have reached a level where it is unclear today what parts of the Internet are not compromised to an extent," he said.

Another interesting measure of the growth of online crime is data showing that criminal groups have shifted their activities from nights and weekends to weekday attacks, suggesting that online crime is evolving into a full-time profession for many.

Criminals also are getting more sophisticated in evading anti-fraud efforts. This year saw the advent and wide deployment of Web-browser based "toolbars" and other technologies designed to detect when users have visited a known or suspected phishing Web site. In response, many online scam artists place phishing Web sites targeting multiple banks and e-commerce companies on the same Web servers, then route traffic to those servers through home computers that they have commandeered with bot programs.

In such operations, each individual scam page is assigned to a Web site that, for a short time, is tied to an Internet address of a compromised computer that the criminals control. When a would-be victim clicks on a link in a phishing e-mail, he or she is routed through the drone PC to the correct scam page. The result is that even if law enforcement or security experts take down the infected PC responsible for relaying traffic to one of the scam sites, the effect of that takedown is only temporary, as the attackers can simply substitute another computer they have gained control over. Such scams make it far more difficult for security experts to find the true location of phishing servers.

The number of phishing scams spotted online exploded during the month of October -- a record 37,444, according to the Anti-Phishing Working Group, an industry coalition aimed at stamping out online fraud. That's 12,000 more phishing sites than were spotted in August, and nine times as many phishing sites as were discovered in October 2005.

Hubbard predicts that 2007 will see the evolution of malware designed to take advantage of presently unknown security holes in browser-based anti-phishing toolbar programs, such as the ones embedded in Mozilla's Firefox 2.0 browser and Microsoft's Internet Explorer Version 7.

Online fraud will get even more sophisticated in 2007, researchers fear. "Criminals have gone from trying to hit as many machines as possible to focusing on techniques that allow them to remain undetected on infected machines longer," said Vincent Weafer, director of security response at the Internet security firm Symantec.
